

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

SENDERRA RX PARTNERS, LLC,
a Texas limited liability company,

Plaintiff,

v.

Case No. 15-13761

DENAY R. LOFTIN and
ELIZABETH R. NAYLOR,

HON. AVERN COHN

Defendants.

**DECISION AND ORDER GRANTING IN PART DEFENDANTS' MOTION FOR
JUDGMENT ON THE PLEADINGS (Doc. 61) AND DISMISSING CASE**

I. Introduction

This is an employment dispute. Plaintiff Senderra RX Partners, LLC (Senderra) is suing two former employees Denay R. Loftin (Loftin) and Elizabeth Naylor (Naylor), collectively "defendants" where appropriate.¹ The complaint essentially boils down to the allegation that defendants took confidential business information and protected patient health information by diverting all of their work emails to third-party email accounts. Senderra says this conduct violates several state and federal laws. The complaint asserts nine (9) claims:

Count I - violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, et seq

¹Naylor has since filed for bankruptcy. Senderra filed an adversary proceeding in Naylor's bankruptcy case. The bankruptcy proceedings have been stayed pending the outcome of the instant motion.

Count II - violation of the Stored Communications Act (SCA), 18 U.S.C. § 2707

Count III - violation of the Electronic Communications Privacy Act (ECPA), in violation of 18 U.S.C. § 2510

Count IV - violation of Michigan's Uniform Trade Secrets Act, M.C.L. § 445.1901, et seq.

Count V - breach of fiduciary duty/duty of loyalty

Count VI - common law and statutory, M.C.L. 600.2919(A) conversion

Count VII - tortious interference with business relationships and expectancies

Count VIII - civil conspiracy

Count IX - negligence

Before the Court is defendants' motion for judgment on the pleadings, contending that all of the claims should be dismissed.² For the reasons that follow, the motion will be granted in part and denied in part. Senderra's federal claims under Counts I, II, and III will be dismissed for failure to state plausible claims for relief. The remaining counts will be dismissed without prejudice because the Court declines to exercise supplemental jurisdiction over them.

II. Background

Following are the relevant facts alleged in the complaint.

Senderra is a Texas limited liability company based in Richardson, Texas. It has offices and operations in Flint, Michigan and is authorized to do business in Michigan. Senderra is a specialty pharmacy serving patients with ailments such as rheumatoid

²This case has been marred by contentious discovery disputes. The Court has stayed discovery until further order following the filing of the motion for judgment on the pleadings. See Doc. 65.

arthritis, psoriasis, osteoporosis, and multiple sclerosis. Senderra's staff assists patients with all aspects of their specialty medications, and coordinates with physicians, insurance providers, and other resources to provide patients with care.

Loftin is a resident of Waterford, Michigan and is a licensed practical nurse ("LPN"), licensed by the State of Michigan. Loftin was employed with Senderra in Flint, Michigan from on or about April 22, 2014, until January 15, 2015.

Naylor is also a resident of Waterford, Michigan and Loftin's sister. She began her employment with Senderra in Flint on or about May 19, 2014, as a receptionist, later moving to the position of Prior Authorization Specialist. She was employed with Senderra from about May 19, 2014, to October 2, 2015.

As an LPN Nurse Consultant and a Prior Authorization Specialist, Loftin and Naylor, respectively, beginning with their training and ongoing throughout their employment, were exposed regularly, in the course of their duties, to proprietary and confidential information, processes, and procedures of Senderra. As part of this exposure and training, Loftin and Naylor also received protected health information, including, but not limited to, medical records and other documents or information that reflect patient names, home addresses, dates of birth, medical diagnoses, prescriptions from doctors, refill orders, specific brands or types of prescription medication, including amounts of same, physician recommendations, and the identities of physicians with whom Senderra has established relationships. They also received training and became familiar with Senderra's highly confidential processes and procedures related to workflow. Senderra also has formal policies governing the protection of confidential and protected patient health information.

During the course of her employment, Loftin set up an auto-forwarding command, rule or feature on her Senderra e-mail account, which directed all e-mails sent to her Senderra e-mail account to be immediately and contemporaneously forwarded to one or more personal e-mail addresses she owned and/or to which she had access. Loftin says this was done with assistance from Senderra's information technology department in order to enable her to work from home. Senderra says that Loftin may have continued to receive emails sent to her Senderra e-mail address because neither Senderra nor Loftin appears to have disabled the forwarding feature at the time of her separation.

During the course of her employment, Naylor also set up an auto-forwarding command, rule or feature on her Senderra e-mail account, which directed all e-mails sent to her Senderra e-mail account to be immediately and contemporaneously forwarded to one or more personal e-mail addresses she owned and/or to which she had access, including her personal email address. Naylor too says that this was done in order to enable her to work from home.

In late August 2015, Senderra says it discovered Naylor's auto forward command and disabled the command through its information technology staff. Senderra later became aware that Loftin had also been forwarding e-mails from her work e-mail to a personal e-mail account. Eventually, Senderra terminated defendants.

III. Legal Standard

The standard of review under Rule 12(c) for judgment on the pleadings is the same as for Rule 12(b)(6). Jelovsek v. Bredesen, 545 F.3d 431, 434 (6th Cir. 2008)

(internal citations omitted). A Rule 12(b)(6) motion tests the sufficiency of a plaintiff's pleading. The Rule requires that a complaint "contain something more . . . than . . . a statement of facts that merely creates a suspicion [of] a legally cognizable right of action." Bell Atlantic Corp. v. Twombly, 550 U.S. 544 (2007)(internal citation omitted). A "plaintiff's obligation to provide the 'grounds' of his 'entitlement to relief' requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." Id. "[T]hat a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions. Threadbare recitals of all the elements of a cause of action, supported by mere conclusory statements do not suffice." Ashcroft v. Iqbal, 556 U.S. 662; 129 S. Ct. 1937, 1949 (2009). The court is "not bound to accept as true a legal conclusion couched as a factual allegation."

IV. Analysis

A. Count I - Computer Fraud and Abuse Act

Under the Computer Fraud and Abuse Act ("CFAA"), Senderra must show the Defendants: (1) accessed a protected computer; (2) without authorization or exceeded authorized access; and (3) there was damage or loss to plaintiff of more than \$5,000 of value in a one-year period. 18 U.S.C. 1030(a)(2); see also Am. Furukawa, Inc. v. Hossain, 103 F. Supp. 3d 864, 871 (E.D. Mich. 2015).³

³Senderra cited American Furukawa at the hearing as support for its claim under the CFAA. Although the district court in American Furukawa found that the complaint stated a claim under the CFAA, the facts alleged here are distinguishable. In American Furukawa, the defendant downloaded company files and emails to his personal computer while on medical leave. Company policy prohibited defendant from accessing any documents while on leave and defendant was instructed "not to work" while on leave. The defendant was also alleged to have used the downloaded information in seeking and obtaining employment with a competitor while on medical leave. This

Accepting Senderra's allegations as true, defendants contend that the complaint fails to sufficiently plead that defendants alleged email forwarding was done without authorization or exceeding access. There is a circuit split on the meaning of "exceeded authorized access." The split centers on whether the terms "without authorization" under the CFAA should be interpreted broadly or narrowly. Under a broad interpretation, a party accesses a computer "without authorization" if he violates the computer's terms of use, or breaches a duty of loyalty. Ajuba Int'l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 686 (E.D. Mich. 2012). Under the narrow interpretation, "an employee's misuse or misappropriation of an employer's business information is not 'without authorization' so long as the employer has given the employee permission to access such information." Id.

Courts in this district have adopted the narrow interpretation. See Ajuba Int'l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 687 (E.D. Mich. 2012) ("Accordingly, a violation for accessing 'without authorization' under the CFAA occurs only where initial access is not permitted and a violation for 'exceeding authorized access' occurs only where initial access is permitted but the access of certain information is not permitted."); Am. Furukawa, Inc. v. Hossain, 103 F. Supp. 3d 864, 873 (E.D. Mich. 2015) ("The Court agrees with the other courts in this district who have adopted the 'narrow' approach to give meaning to the CFAA's 'without authorization' language."). Other district courts in this Circuit have likewise read the statute narrowly. See Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc., No. 1:10-CV-450, 2012 WL 2524008 (W.D. Mich. June 29, 2012);

factual scenario is far different from the auto-forwarding of emails at issue in the instant case.

ReMedPar, Inc. v. AllParts Med., L.L.C., 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010); Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929 (W.D. Tenn. 2008).

Indeed, the Sixth Circuit has said that if an employee has been granted access to the information, the employee is not “exceeding access” even if the information is misused. See Ajuba Int’l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 685-86 (E.D. Mich. 2012) (citing LVRC Holdings L.L.C. v. Brekka, 581 F.3d 1127 (9th Cir. 2009); Orbit One Commc’ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010)).

Here, Senderra alleges that throughout defendants’ employment, defendants both had authorized access to their email accounts, so any emails sent to defendants during their employment would be within their authorized access. (Doc. 1, Complaint at ¶ 22, 24). In terms of any unauthorized access, Senderra only asserts one of the defendants, Loftin, “may have continued to receive emails” after her termination. Complaint at ¶ 27. Senderra offers no facts supporting the statement that Loftin received any emails after her termination. If Loftin did receive emails to her personal account after termination, as alleged, it was because Senderra failed to disable her company email address. If Senderra failed to disable or redirect Loftin’s Senderra email, Senderra did not revoke access.

Under the CFAA “once an employee is granted ‘authorization’ to access an employer's computer that stores confidential company data, that employee does not violate the CFAA regardless of how he subsequently uses the information.” Ajuba Int’l, L.L.C. v. Saharia, 871 F. Supp. 2d 671, 686 (E.D. Mich. 2012). Defendants could not have conspired to set-up an auto-forwarding function in violation of the CFAA because defendants were authorized to access Senderra computer data.

Senderra has also not sufficiently plead that defendants accessed a protected computer. Senderra alleges that defendants' emails were forwarded to third-party email addresses. Complaint at ¶ 28-29. For these reasons, the complaint fails to allege a plausible claim under the CFAA.

Additionally, Senderra's claims under the CFAA is inappropriate because the CFAA was not enacted to be used against employees who take or misuse information, it was enacted to punish hackers. Am. Family Mut. Ins. Co. v. Rickman, 554 F. Supp. 2d 766, 771 (N.D. Ohio 2008) ("The statute was not meant to cover the disloyal employee who walks off with confidential information. Rather, the statutory purpose is to punish trespassers and hackers."). Defendants alleged forwarding of Senderra emails simply does not come within the confines or purpose of the CFAA. Count I must be dismissed.

B. Count II - Stored Communications Act

Under the Stored Communications Act ("SCA"), it is punishable when a person "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701 (a); see also Cobra Pipeline Co. v. Gas Nat., Inc., 132 F. Supp. 3d 945, 949 (N.D. Ohio 2015). An exception exists whereby a communication "intended for that user" is not punishable. 18 U.S.C. § 2701 (c)(2).

Defendants contend that they fall under the user exception to the SCA because all of the emails they received were intended for them. The Court agrees. All of the emails Senderra contends the defendants received were sent to an email address

connected directly to the defendant's name and email account, whether the account was at Senderra or with a third party. Even Senderra admits to the fact that any emails forwarded to Defendants' personal email addresses were "sent to [Defendants] Senderra e-mail account." Complaint at ¶ 25. Therefore, all emails Senderra contends were in violation of the SCA fit into the user exception because only the person the email was intended for was accessing the email. Anything defendants did with their authorized access to Senderra email does not fall under the CFAA.

Senderra, however, says that defendants do not fit under the user exception. The Court disagrees. As explained by the Court of Appeals for the Ninth Circuit, "[t]he SCA excepts from liability, however, 'conduct authorized ... by a **user** of that service with respect to a communication of or intended for that user.' 18 U.S.C. § 2701(c)(2)." (emphasis added)). Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002). Defendants fit into the intended user exception because the emails were sent to defendants and clearly intended for defendants, making Defendants the "user." Contrary to Senderra's argument, the intended user exception is not related to the company that provides the email address, i.e. Senderra. The Ninth Circuit has also found "legislative history that Congress believed 'addressees' or 'intended recipients' of electronic communications would have the authority under the SCA to allow third parties access to those communications." See id. at 880.

Even if the defendants did not fit into the user exception, defendants say that they did not access a "facility," as required for liability under the SCA. The Court agrees. Defendants would have been viewing any forwarded emails through their personal computers and cell phones. Although courts are not in agreement as to

exactly what “facility” means, many agree a “facility” does not include a computer or phone. See Lazette v. Kulmatycki, 949 F. Supp. 2d 748, 756 (N.D. Ohio 2013) (“the better, more sensible, and harmonious reading of the SCA is that a personal computer, and, ergo, a blackberry or cell phone, is not a ‘facility’ within § 2701(a)(1).”); Garcia v. City of Laredo, Texas, 702 F.3d 788, 792 (5th Cir. 2012) (“the relevant ‘facilities’ that the SCA is designed to protect are not computers that enable the use of an electronic communication service, but instead are facilities that are operated by electronic communication service providers and used to store and maintain electronic storage.” (citation omitted) (emphasis added)); In re iPhone Application Litigation, 844 F. Supp. 2d 1040, 1057-1058 (N.D. Cal. 2012) (“Plaintiffs fail to state a claim under the SCA because their iOS devices do not constitute ‘facilit[ies] through which an electronic communication service is provided.’”).

Here, Senderra does not contend that defendants did anything more than access their personal email addresses on their personal devices after emails were forwarded to them from their own Senderra email accounts. See Complaint at ¶¶ 31-40. Therefore, Senderra has not stated a claim that defendants are liable under the SCA.

C. Count III - Electronic Communications Privacy Act

18 U.S.C. § 2511 is a provision of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2520, also known as the federal “Wiretap Act.” The Wiretap Act was partially revised by Title I of the Electronic Communications Privacy Act of 1986.

Section 2511(1)(a) makes it punishable when a person “intentionally intercepts, endeavors to intercept, or procures any other person to intercepts or endeavor to

intercept, any . . . electronic communication.”

Section 2511(1)(c) provides:

any person who ... intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection ... shall be subject to suit as provided in subsection (5).

Thus, for defendants to have violated section 2511(1)(a) or 2511(1)(c), they must have:

- (1) intentionally intercepted an electronic communication, or
- (2) intentionally disclosed an electronic communication that they knew or had reason to know was intercepted in violation of section 2511.

Additionally, under section 2511(d), interception can occur by one who is a party to the communication if the communication is intercepted “for the purpose of committing any criminal or tortious act...” In other words, if defendants intercepted an email for purposes of committing a criminal act or a tort, the fact that they were a party to the email would not matter.

Here, the conduct alleged in the complaint does not constitute an intercept. The statute defines an “intercept” as the an “aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.”

As one district court put it:

Though, in layman's terms, the act of accessing and forwarding an e-mail from another's e-mail account could be understood as an “intercept,” cases interpreting this term have given the word a much narrower definition.

Frederick v. Oldham Cty. Fiscal Court, 2010 WL 2572815 (W.D. Ky. June 23, 2010).

As the courts have interpreted In other words, an email can only be “intercepted”

if it is accessed before it gets to the intended recipient. Accessing an email that has been sent and is in storage is not an intercept. Here, nothing happened during the time in which the emails were sent from Senderra to defendants - who were the intended recipients. The fact that the emails are alleged to have been later forwarded by defendants to another email account simply does not describe the type of conduct which falls under the ECPA. Again, Senderra admits any emails auto-forwarded to Defendants' personal email addresses were "sent to [Defendants] Senderra e-mail account." Complaint at ¶ 25. Merely accessing email through an account or server after it has been received simply does not rise to a plausible violation of the statute. See Fredrick, supra at *3 (W.D. Ky. June 23, 2010) ("Thus, interception includes accessing messages in transient storage on a server during the course of transmission, but does not include accessing the messages stored on a destination server." (citation omitted)).

D. State Law Claims

The remaining claims are all based on state law. While the parties spend a good deal of time arguing over whether they are properly plead, it is neither necessary or appropriate to consider whether these state law claims are viable as explained below.

Federal district courts have original subject-matter jurisdiction over cases arising under federal law. 28 U.S.C. § 1331. As such, the Court has subject-matter jurisdiction over Counts I, II, and III. The remaining counts, Counts IV - IX, are state law claims. Although the Court has supplemental jurisdiction over these state-law claims under 28 U.S.C. § 1367(a),⁴ it may decline to exercise supplemental jurisdiction if the state-law

⁴28 U.S.C. § 1367 provides that "the district court shall have supplemental jurisdiction over all other claims that are so related to the claims in the action within

claim “substantially predominates over the claim or claims over which the district court has original jurisdiction,” or if “there are other compelling reasons for declining jurisdiction.” Id. § 1367(c)(2), (c)(4).

Where, as here, federal claims have been dismissed on the merits, the question of whether to retain jurisdiction over the state law claims rests within the Court's discretion. Blakely v. United States, 276 F.3d 853, 860 (6th Cir.2002); Weeks v. Portage County Executive Offices, 235 F.3d 275, 280 (6th Cir.2000) (observing that section 1367(c) “permit[s] the district court to decline to exercise supplemental jurisdiction when that court has dismissed all of the claims over which it has original jurisdiction”). As a general rule, the dismissal of claims over which the federal court had original jurisdiction creates a presumption in favor of dismissing without prejudice any state-law claims that accompanied it to federal court. Blakely, 276 F.3d at 863. See also United Mine Workers of Am. v. Gibbs, 383 U.S. 715, 726 (1966); Brooks v. Rothe, 577 F.3d 701, 709 (6th Cir. 2009).

Here, because the federal claims are subject to dismissal, and as this case is before this Court only on federal question jurisdiction, the Court will decline supplemental jurisdiction over the remaining state law claims. It is particularly appropriate because the state law claims substantially predominate over the federal claims and raise novel and complex issues of state law that would be more appropriately adjudicated by the state court. See § 1367(c) (1), (c)(4); Padilla v. City of Saginaw, 867 F. Supp. 1309, 1315 (E.D. Mich.1994).

such original jurisdiction that they form a part of the same case or controversy.” 28 U.S.C. § 1367(a)

V. Conclusion

For the reasons stated above, defendants' motion is GRANTED IN PART AND DENIED IN PART. Counts I, II, and III are DISMISSED WITH PREJUDICE. Counts IV-IX are DISMISSED WITHOUT PREJUDICE. This case is DISMISSED.

SO ORDERED.

S/Avern Cohn
AVERN COHN
UNITED STATES DISTRICT JUDGE

Dated: December 8, 2016
Detroit, Michigan